UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Diretoria de Infraestrutura e Suporte ao Usuário
Av. João Naves de Ávila, 2121, Bloco 1J - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4319 - operacao@cti.ufu.br

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Registro de preços para aquisição de *firewalls* de pequeno porte, *firewalls* de médio porte e analisador de tráfego, armazenamento de *log* e relatórios conforme condições, quantidades, exigências e estimativas estabelecidas neste instrumento.

1.2. Em conformidade com o art 1.º da Lei 10.520/202 e Decreto 10.024/2019, o objeto pretendido enquadra-se como “bem comum” por apresentar, independente de sua complexidade, “padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado”.

1.3. De acordo com o Inc. III do art 6.º da Lei 8.666/93, enquadra-se no tipo Compra, por envolver a “aquisição remunerada de bens para fornecimento de uma só vez ou parceladamente”.

1.4. A itens a seguir, objetos desta contratação, não incidem nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD/ME nº 1/2019.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. A solução de TIC é composta pelos bens e serviços indicados na tabela a seguir:

Id.	Descrição do Bem	Código CATMAT	Quantidade	Métrica ou Unidade
1	Firewall de médio porte com suporte e garantia de 60 meses	150100	11	Unidade
2	Firewall de pequeno porte com suporte e garantia de 60 meses	150100	12	Unidade
3	Analisador de tráfego, armazenamento de log e relatórios com suporte e garantia de 60 meses	150100	1	Unidade

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. A Universidade Federal de Uberlândia possui uma extensa estrutura de rede de dados, baseada no padrão Ethernet, em que várias edificações são interligadas utilizando a topologia estrela dentro de cada campus da universidade.

3.1.2. Nestes campi existem os denominados datacenters, os quais concentram as fibras ópticas oriundas das edificações e ligadas a equipamentos de comutação de dados (switches) com portas para as fibras ópticas. Nos casos específicos dos campi Santa Mônica e Umuarama, devido à alta concentração predial e outros ativos de rede, são requeridos equipamentos com maior densidade de portas para fibra óptica, denominados switches core.

3.1.3. Em cada campus, a UFU possui um link de dados fornecido pela RNP (Rede Nacional de Ensino e Pesquisa), conforme detalhado na Figura 1, a partir do qual tem-se o acesso a internet. Além destes links, temos links contratados pela própria UFU fornecendo conectividade direta entre os campi para acesso a serviços e sistemas internos.

3.1.4. Cada campus, exposto à internet pela link da RNP, deve ser capaz de se proteger de tentativas de ataques cada vez mais comuns, especialmente no setor público, conforme notícias recentes [1,2,3,4] divulgadas em jornais e revistas especializadas.

3.1.5. Para prover tais proteções, devem ser utilizadas ferramentas denominadas firewalls, protegendo contra diversos tipos de ataques externos. Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas (protegidas e controladas) e redes externas, confiáveis ou não, como a Internet. Um firewall pode ser um hardware, software ou ambos.

3.1.6. Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.

3.1.7. De acordo com a definição do Gartner, Inc., um firewall de próxima geração deve incluir:

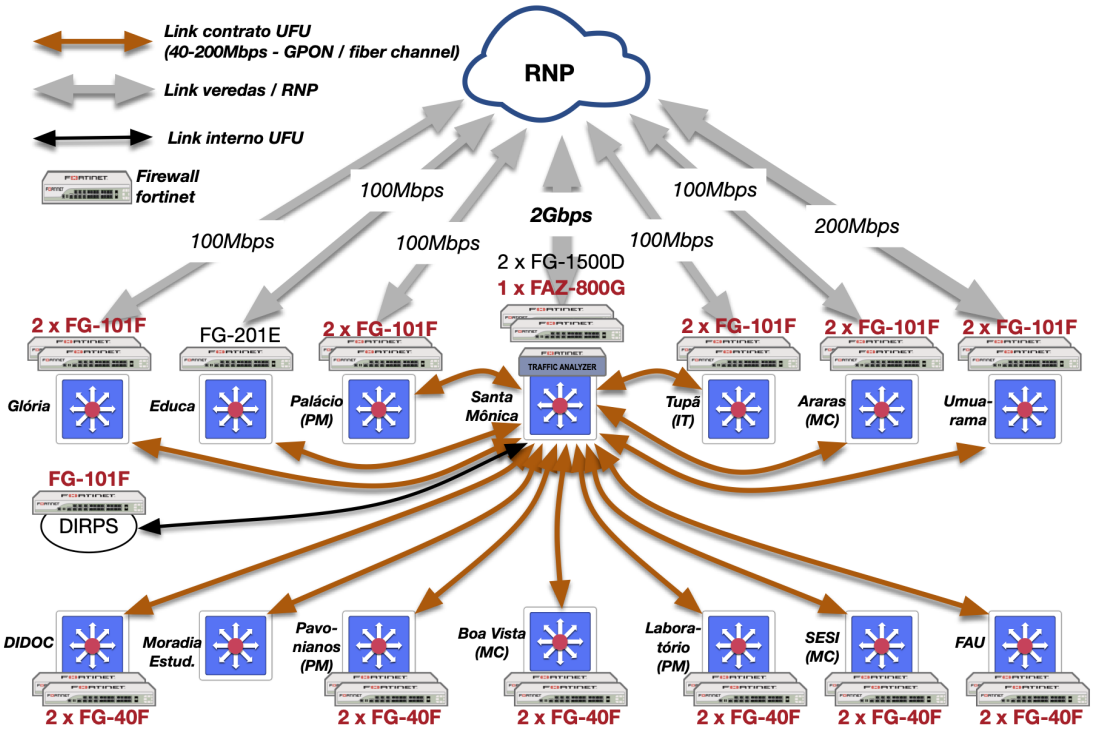
- Recursos padrão de firewall, como inspeção stateful
- Prevenção de invasão integrada
- Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos Atualização de caminhos para incluir feeds futuros de informação
- Técnicas para lidar com as ameaças à segurança em evolução

3.1.8. Atualmente, a UFU conta com este tipo de firewall de próxima geração apenas em dois campi, Santa Mônica e Ituiutaba. Os demais campi contam apenas com proteções básicas de entrada e saída por porta de acesso através de firewall iptables/pfsense.

3.1.9. O objetivo deste estudo é prover o levantamento necessário para equipar todos os campi da UFU com equipamentos de firewall de próxima geração, aumentando a segurança e tolerância a ataques, protegendo os sistemas e serviços da própria universidade, bem como o próprio parque computacional utilizado pela comunidade acadêmica.

3.1.10. Para garantir, além da segurança adequada, alta disponibilidade no fornecimento de serviço de conectividade, faz-se necessária ainda a utilização destes equipamentos de firewall em uma estrutura de alta disponibilidade, ou seja, ao menos dois equipamentos por campus, de tal modo que a falha de um não interrompa o funcionamento da rede.

3.1.11. A Figura 2 do Estudo Técnico Preliminar (ETP) presente neste processo e apresentada a seguir, ilustra o cenário final pretendido como resultado desta contratação. Cada campus avançado e escritório da Universidade contaria com um par de equipamentos de firewall. Neste cenário, devido à diversidade dos serviços, taxa de utilização dos links e quantidade de usuários, pretende-se adquirir dois modelos de firewall. Neste cenário teríamos 5 (cinco) campi com 2 firewalls de médio porte instalados em alta disponibilidade, ou seja, 2 (dois) equipamentos por campus, e mais 1 (um) equipamento na Diretoria de Processos Seletivos (DIRPS), devido à sensibilidade dos dados manuseados por esta diretoria, tais como dados de inscrição de processos seletivos, notas e classificação de candidatos. Além disso, 6 (seis) campi/escritórios menores receberia 2 (dois) firewalls de pequeno porte cada, totalizando mais 12 (doze) equipamentos.



3.1.12. Neste mesmo ambiente, é importante que haja a figura de uma entidade centralizadora capaz de monitorar em tempo real o tráfego passando por cada firewall, detectando de maneira pró-ativa possíveis ataques e sugerindo modificações e/ou otimizações no controle de acesso à rede. Este equipamento, denominado analisador de tráfego de rede, ou simplesmente *analyzer*, deve ser robusto o suficiente para processar bilhões de entradas nos registros de cada firewall por dia.

3.2. **Alinhamento aos Instrumentos de Planejamento Institucionais**

3.2.1. A presente contratação está prevista no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para o período 2021/2022, bem como no Plano Anual de Contratações (PAC) 2022 da Universidade Federal de Uberlândia, conforme detalhado a seguir.

3.2.1.1. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2021-2022**: *Meta STIC 03 - Appliance de Segurança para a Rede UFU (Firewall)*

3.2.1.2. **Alinhamento PAC:** *Item 2248 - Código 150100 - FIREWALL*

3.3. **Estimativa da Demanda**

3.3.1. Visando uma instalação escalonada, principalmente no sentido de interrupção mínima dos serviços e sistemas em operação e adequação das atividades à força de trabalho disponível no Centro de Tecnologia da Informação e Comunicação (CTIC), órgão responsável pela gerência de toda a infraestrutura de rede da Universidade, este documento recomenda a aquisição dos equipamentos e sua instalação em duas etapas.

3.3.2. A etapa inicial, executada ainda este ano, compreende a instalação e configuração de um firewall de médio porte em cada campus avançado - Glória, Palácio (PM), Tupã (IT), Araras (MC) e Umuarama (UM) -, bem como na Diretoria de Processos Seletivos (DIRPS). O equipamento atualmente instalado em Ituiutaba (FG-201E) será reinstalado no Campus Educa.

3.3.3. A instalação em cada campus garante a proteção e monitoramento adequados. A DIRPS também é uma prioridade devido à
grande exposição à comunidade externa como ponto de entrada na Universidade.

3.3.4. **Nesta primeira etapa**, temos os seguintes quantitativos por equipamento:

- Firewall de médio porte (FG-101F): 6 (seis) unidades;
- Analisador e armazenamento de logs (FAZ-800G): 1 (uma) unidade.

3.3.5. A segunda etapa compreende a disponibilização dos cinco campi da primeira etapa em alta disponibilidade (HA - High Availability) para tolerar falhas, além de 6 (seis) outros locais menores com firewall de pequeno porte, também em HA. A Figura anterior representa o cenário desejado ao final da contratação. Esta configuração prevê *appliances* de firewall em todos os campi e escritórios da UFU, em HA, oferecendo segurança completa, controle e acompanhamento de uso por meio do analisador de tráfego.

3.3.6. **Na segunda etapa**, temos os seguintes quantitativos por equipamento:

- Firewall de médio porte (FG-101F): 5 (cinco) unidades;
- Firewall de pequeno porte (FG-40F): 12 (doze) unidades.

3.3.7. Deste modo, **ao final de todas as etapas**, teremos os seguintes quantitativos por equipamento:

- Firewall de médio porte (FG-101F): 11 (onze) unidades (6 da primeira etapa somados a 5 da segunda etapa);
- Firewall de pequeno porte (FG-40F): 12 (doze) unidades (segunda etapa);
- Analisador e armazenamento de logs (FAZ-800G): 1 (uma) unidade (primeira etapa).

3.4. **Adesões à Ata de Registro de Preços (ARP)**

3.4.1. O lançamento da Intenção de Registro de Preços requer redução na celeridade do processo visando uma possível economia de escala. Entretanto, é possível a permissão de adesões à ARP após sua conclusão, o que gera economia nas contratações dos órgãos interessados em participar desta ata. Buscando-se um equilíbrio nessa balança de economias a serem geradas pela Administração, a UFU prioriza a adesão à ARP à adesão à IRP buscando uma economia no processo, tanto para o órgão gerenciador, quanto para o não participante.

3.5. **Parcelamento da Solução de TIC**

3.5.1. O Art. 23, §1º, da Lei 8666, de 1993, determina que as obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade sem perda da economia de escala.

3.5.2. Adicionalmente, a Súmula TCU nº 247 dispõe que é obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

3.5.3. A solução em questão representa a aquisição de ativos de TIC para aumentar a segurança na infraestrutura de redes e serviços da Universidade Federal de Uberlândia. O parcelamento da entrega de 1 único equipamento não é viável, pois o funcionamento do mesmo depende de todo o conjunto de peças fornecido internamente bem como do software vinculado ao mesmo.

3.6. **Resultados e Benefícios a Serem Alcançados**

3.6.1. Os resultados pretendidos são:

3.6.1.1. Aumento na segurança da rede interna da Universidade em todos os campi.

3.6.1.2. Monitoramento de usuários, equipamentos e aplicações quanto a atividades maliciosas.

3.6.1.3. Inspeção de pacotes no nível de conexões, e não simplesmente pacotes individuais.

3.6.1.4. Melhoria no fornecimento de acesso seguro à rede interna da Universidade, especialmente com a implantação do

trabalho remoto.

3.6.1.5. Maior controle de aplicações e sistemas com definição de regras específicas para cada situação.

3.6.1.6. Bloqueio automatizado de tentativas de intrusão com impedimento de qualquer acesso futuro a partir da fonte do ataque.

3.6.1.7. Aprendizado por meio de inteligência artificial e atualização automatizada de base de dados de ameaças, com
consequente aumento da capacidade de detecção das mesmas.

3.6.1.8. Geração de relatórios avançados em tempo real para ações de fiscalização e melhoria de utilização da infraestrutura de

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Os produtos deverão obedecer às prescrições e exigências contidas nas especificações deste Termo de Referência, o Estudo Técnico Preliminar e seus anexos, bem como todas e quaisquer normas ou regulamentações intrínsecas ao tipo de fornecimento.

4.1.2. O item fornecido deve ser novo e estar em perfeitas condições de uso e funcionamento, não sendo aceito, em hipótese alguma, materiais recondicionados, ou, ainda, que não atendam integralmente as especificações técnicas e condições aqui estabelecidas e em desacordo com as normas pertinentes.

4.2. Requisitos de Capacitação

4.2.1. O Centro de Tecnologia da Informação e Comunicação (CTIC) da UFU conta com equipe de analistas aptos à instalação e configuração dos equipamentos objetos desta contratação, não havendo, portanto, necessidade de capacitação.

4.3. Requisitos Legais

4.3.1. Considerando as características do objetivo, cujos padrões de desempenho e qualidade permitem definições objetivas com base em especificações usuais de mercado, o processo licitatório deve ser realizado na modalidade Pregão, do tipo Menor Preço, na forma eletrônica, conforme estabelecido no Decreto nº 7.174, de 12 de maio de 2010, nas demais legislações pertinentes, a saber: Lei nº 10.520 de 17 de julho de 2002, Lei nº 8.248 de 23 de outubro de 1991, Lei nº 13.709 de 14 de agosto de 2018, Decreto nº 10.024 de 20 de setembro de 2019, Decreto nº 7.746 de 05 de junho de 2012, Instrução Normativa SGD/ME nº 01 de 04 de abril de 2019, Instrução Normativa SEGES/MP nº 03 de 26 de abril de 2018, Lei Complementar nº 123 de 14 de dezembro de 2006, Decreto nº 8.538 de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666 de 21 de junho de 1993.

4.3.2. A presente contratação segue modelos definidos pela IN SGD/ME nº 1/2019 em seu artigo 8º.

4.4. Requisitos de Suporte Técnico e Manutenção

4.4.1. Da atualização

4.4.1.1. A contratada deverá disponibilizar, na vigência da Garantia, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;

4.4.1.2. As atualizações incluídas devem ser do tipo “minor release” e “major release”, permitindo manter os equipamentos atualizados em sua última versão de software/firmware.

4.4.2. Do suporte técnico

4.4.2.1. O suporte técnico deverá ser prestado pela contratada, sendo facultado a esta escalar as questões para o respectivo fabricante.

4.4.2.2. Deverá ser disponibilizada, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, sistema web de helpdesk (sistema de chamados) e e-mail, com disponibilidade para registro e acompanhamento de solicitações.

4.4.2.3. O registro da solicitação pode ser realizado através de contato telefônico, disponibilizado no regime mínimo de 8x5 (8 horas por dia, 5 dias por semana), com o primeiro atendimento em até 4 horas úteis;

4.4.2.4. As ligações deverão ser preferencialmente do tipo gratuitas;

4.4.2.5. A contratada deverá disponibilizar um portal web e/ou número telefônico 0800 (gratuito) com disponibilidade 24x7 (24 horas por dia, 7 dias por semana), com sistema de helpdesk para abertura de chamados de suporte técnico com consulta e acompanhamento em tempo real ao histórico e andamento de atendimentos;

4.4.2.6. Deverá ser disponibilizada facilidade para a equipe técnica da contratante abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico em tempo real.

4.4.2.7. Os chamados abertos por e-mail deverão ser vinculados ao sistema de helpdesk;

4.4.2.8. Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema de helpdesk.

4.4.2.9. A contratada deverá prestar o suporte técnico dos produtos fornecidos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a contratada responsável pelo gerenciamento do chamado e prestação de informações à contratante.

4.4.2.10. A contratada deve indicar os procedimentos para abertura de suporte técnico.

4.4.3. O prazo para troca de peças ou mesmo de todo o equipamento deve ser de até 7 (sete) dias úteis após a abertura do chamado técnico nas dependências da universidade (on-site).

4.5. **Requisitos Temporais**

4.5.1. Prazo de entrega dos produtos deve ocorrer em no máximo 60 (sessenta) dias corridos a partir do recebimento da nota de empenho por parte do fornecedor.

4.5.2. No caso comunicações realizadas via mensagens eletrônicas (e-mail) expedidas pela Contratante, será considerado como data de recebimento (pela Contratada) o dia útil subsequente à data de envio.

4.5.3. O prazo de garantia deve ser de no mínimo 5 (cinco) anos, contado a partir do recebimento definitivo do produto.

4.5.4. O atendimento do chamado em primeiro nível, independente do canal adotado, deve ocorrer em até 24 horas.

4.5.5. Durante o período de garantia, o prazo para substituição de materiais, por rejeição, defeito, vícios ou incorreções, será de no máximo 7 (sete) dias úteis, contados a partir do dia subsequente à notificação à contratante, independente do canal adotado.

4.5.6. O recebimento definitivo e ateste da nota fiscal deve ocorrer em até 15 dias corridos a contar da data do recebimento provisório.

4.5.7. Os itens devem ser entregues no endereço da Divisão de Recepção, Armazenagem e Distribuição de Equipamentos da Universidade Federal de Uberlândia, na Av. Amazonas, 2210 - Bloco 2Z - Sala(s) DIRAM - Bairro Umuarama - Campus Umuarama - Uberlândia-MG - CEP 38405-302.

4.5.8. A entrega deve ser feita em duas parcelas, sendo uma parcela para cada etapa, conforme etapas e quantidades detalhadas no **subitem 3.3**.

4.5.9. O **cronograma de entrega** será feito por etapa detalhada no **subitem 3.3,** conforme calendário a seguir:

4.5.9.1. Etapa um: entrega até dezembro de 2022.

4.5.9.2. Etapa dois: entrega até julho de 2023.

4.6. **Requisitos de Segurança**

4.6.1. Um dos requisitos básicos para a segurança do hardware é o isolamento físico dos equipamentos e o controle de acesso.

4.6.2. O acesso aos equipamentos deverá ser restrito às pessoas autorizadas e capacitadas, incluindo os gestores e técnicos responsáveis pela manutenção e instalação dos equipamentos, evitando assim o acesso indevido, diminuindo os furtos e possíveis danos pela eventual má utilização dos mesmos.

4.6.3. A instalação, utilização e manutenção dos equipamentos deverá obedecer às normas de segurança vigentes. Além disso, deverão estar de acordo com as instruções do fabricante em relação ao transporte, armazenamento, instalação e utilização.

4.6.4. A Solução deve estar em conformidade com a diretiva RoHS.

4.7. **Requisitos Sociais, Ambientais e Culturais**

4.7.1. A contratada para fornecimento dos equipamentos deverá:

4.7.1.1. observar, no que couber, às exigências de sustentabilidade ambiental estabelecidas na Instrução Normativa no 01/2010 da SLTI/MPOG, de 19 de janeiro de 2010, bem como o Decreto no 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável;

4.7.1.2. cumprir, no que couber, as exigências do inciso XI, art. 7o da Lei 12.305, de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS. 20.3;

4.7.1.3. cumprir, no que couber, as exigências do art. 6o da Instrução Normativa MPOG no 01, de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços.

4.8. **Requisitos de Arquitetura Tecnológica**

4.8.1. **ITEM 1 - FIREWALL DE MÉDIO PORTE**

4.8.1.1. **Descrições básicas**

4.8.1.1.1. Throughput de, no mínimo, 1.6 Gbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação, habilitadas simultaneamente;

4.8.1.1.2. Throughput de, no mínimo, 1 Gbps para Prevenção de ameaças, considerando Controle de Aplicação, IPS, anti malware e firewall, habilitados simultaneamente;

4.8.1.1.3. Throughput de, no mínimo, 20 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

4.8.1.1.4. Suporte a, pelo menos, 1.5 milhões de sessões concorrentes TCP;

4.8.1.1.5. Suporte a, pelo menos, 56 mil novas sessões TCP por segundo;

4.8.1.1.6. Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

4.8.1.1.7. Throughput de, no mínimo, 2.6 Gbps de IPS;

4.8.1.1.8. Suporte a, no mínimo, 500 clientes VPN SSL;

4.8.1.1.9. Suporte a, no mínimo, 500 clientes VPN IPsec;

4.8.1.1.10. Possuir ao menos 2 interfaces SFP+ e 12 interfaces RJ45 padrão Gigabit Ethernet;

4.8.1.1.11. Suportar a criação de no mínimo 5 instâncias virtuais;

4.8.1.1.12. Deve suportar a instalação em rack padrão 19”;

4.8.1.1.13. Possuir alimentação elétrica redundante de corrente alternada padrão 110v/220v (fontes redundantes);

4.8.1.1.14. Possuir disco de estado sólido local que suporte ao menos 480 GB de dados;

4.8.1.1.15. Deve estar homologado na ANATEL até a data da licitação;

4.8.1.1.16. Os números acima devem ser comprovados com documentação pública, disponível no site do fabricante.

4.8.1.2. **Características Gerais**

4.8.1.2.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

4.8.1.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

4.8.1.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.8.1.2.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.8.1.2.5. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

4.8.1.2.6. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

4.8.1.2.7. Deve suportar BGP, OSPF, RIP e roteamento estático;

4.8.1.2.8. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

4.8.1.2.9. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

4.8.1.2.10. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;

4.8.1.2.11. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;

4.8.1.2.12. Deve suportar NAT dinâmico (Many-to-Many);

4.8.1.2.13. Deve suportar NAT estático (1-to-1);

4.8.1.2.14. Deve suportar NAT estático bidirecional 1-to-1;

4.8.1.2.15. Deve suportar Tradução de porta (PAT);

4.8.1.2.16. Deve suportar NAT de Origem;

4.8.1.2.17. Deve suportar NAT de Destino;

4.8.1.2.18. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

4.8.1.2.19. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

4.8.1.2.20. Deve suportar NAT64;

4.8.1.2.21. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

4.8.1.2.22. Enviar log para sistemas de monitoração externos;

4.8.1.2.23. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

4.8.1.2.24. Proteção anti-spoofing;

4.8.1.2.25. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

4.8.1.2.26. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.8.1.2.27. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

4.8.1.2.28. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

4.8.1.2.29. Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound);

4.8.1.2.30. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos e softwares a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

4.8.1.2.31. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

4.8.1.2.32. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI;

4.8.1.2.33. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

4.8.1.2.34. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN.

4.8.1.3. **Políticas**

4.8.1.3.1. Deverá suportar controles por zonas de segurança;

4.8.1.3.2. Deverá suportar controles de políticas por porta e protocolo;

4.8.1.3.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

4.8.1.3.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.8.1.3.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

4.8.1.3.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

4.8.1.3.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

4.8.1.3.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

4.8.1.3.9. Suporte a objetos e regras IPV6;

4.8.1.3.10. Suporte a objetos e regras multicast;

4.8.1.3.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré- definidos automaticamente.

4.8.1.4. **Controle de Aplicações**

4.8.1.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.8.1.4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.8.1.4.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.8.1.4.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, twitter, logmein, teamviewer, ms- rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, dropbox, google drive, ldap, radius, itunes, dhcp, ftp, dns, ntp, snmp, webex, evernote, google-docs;

4.8.1.4.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.8.1.4.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.8.1.4.7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.8.1.4.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

4.8.1.4.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.8.1.4.10. Atualizar a base de assinaturas de aplicações automaticamente;

4.8.1.4.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory/LDAP, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

4.8.1.4.12. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.8.1.4.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos;

4.8.1.4.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

4.8.1.4.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.8.1.4.16. Deve alertar o usuário quando uma aplicação for bloqueada;

4.8.1.4.17. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle /políticas para os mesmos;

4.8.1.4.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

4.8.1.4.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo: permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

4.8.1.4.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle /políticas para os mesmos;

4.8.1.4.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

4.8.1.4.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

4.8.1.4.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

4.8.1.4.24. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

4.8.1.4.25. Deve permitir o filtro de vídeos que podem ser visualizados no YouTube.

4.8.1.5. **Prevenção de ameaças**

4.8.1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti- Spyware integrados no próprio appliance de firewall;

4.8.1.5.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.8.1.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.8.1.5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e colocar em quarentena o IP do atacante por um intervalo de tempo;

4.8.1.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.8.1.5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

4.8.1.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.8.1.5.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.8.1.5.9. Deve permitir o bloqueio de vulnerabilidades;

4.8.1.5.10. Deve permitir o bloqueio de exploits conhecidos;

4.8.1.5.11. Deve incluir proteção contra-ataques de negação de serviços;

4.8.1.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

4.8.1.5.13. Detectar e bloquear a origem de portscans;

4.8.1.5.14. Bloquear ataques efetuados por worms conhecidos;

4.8.1.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.8.1.5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.8.1.5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.8.1.5.18. Deve permitir usar operadores lógicos de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

4.8.1.5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.8.1.5.20. Identificar e bloquear comunicação com botnets;

4.8.1.5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.8.1.5.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

4.8.1.5.23. Os eventos devem identificar o país de onde partiu a ameaça;

4.8.1.5.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

4.8.1.5.25. Possuir proteção contra downloads involuntários de arquivos executáveis e maliciosos, usando HTTP;

4.8.1.5.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de

segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.8.1.5.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

4.8.1.5.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

4.8.1.5.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

4.8.1.6. **Filtro de URLs**

4.8.1.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.8.1.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

4.8.1.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory/LDAP e base de dados local;

4.8.1.6.4. A identificação pela base do Active Directory/LDAP deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

4.8.1.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

4.8.1.6.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

4.8.1.6.7. Possuir pelo menos 60 categorias de URLs;

4.8.1.6.8. Deve possuir a função de exclusão de URLs do bloqueio;

4.8.1.6.9. Permitir a customização de página de bloqueio;

4.8.1.6.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

4.8.1.6.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário.

4.8.1.7. **Identificação de usuários**

4.8.1.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

4.8.1.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.8.1.7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

4.8.1.7.4. Deve possuir integração com Microsoft Active Directory/LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

4.8.1.7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em usuários e grupos de usuários;

4.8.1.7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em Usuários e Grupos de usuários;

4.8.1.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

4.8.1.7.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.8.1.7.9. Deve suportar o envio e recebimento de credenciais via RADIUS.

4.8.1.8. **Filtro de dados**

4.8.1.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

4.8.1.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.8.1.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.8.1.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

4.8.1.9. **Geolocalização**

4.8.1.9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado(s) País(es) seja(m) bloqueado(s);

4.8.1.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.8.1.10. **VPN Client to Site**

4.8.1.10.1. Suportar IPSec VPN;

4.8.1.10.2. Suportar SSL VPN;

4.8.1.10.3. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.8.1.10.4. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.8.1.10.5. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

4.8.1.10.6. Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

4.8.1.10.7. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.8.1.10.8. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

4.8.1.10.9. Suportar leitura e verificação de CRL (certificate revocation list);

4.8.1.10.10. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

4.8.1.10.11. A VPN SSL deve permitir aos usuários remotos a troca de senha no Active Directory/LDAP;

4.8.1.10.12. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 e superior).

4.8.1.11. **Recursos Gerais de SD-WAN**

4.8.1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

4.8.1.11.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

4.8.1.11.2.1. Endereços de origem;

4.8.1.11.2.2. Grupos de usuários;

4.8.1.11.2.3. Endereços de destino;

4.8.1.11.2.4. DSCP;

4.8.1.11.2.5. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

4.8.1.11.3. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

4.8.1.11.4. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G;

4.8.1.11.5. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

4.8.1.11.6. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

4.8.1.11.7. A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

4.8.1.11.8. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

4.8.1.11.9. A solução deve permitir a definição do roteamento para cada aplicação;

4.8.1.11.10. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

4.8.1.11.11. Deve possibilitar a definição do link de saída para uma aplicação específica;

4.8.1.11.12. Deve implementar balanceamento de link por hash do IP de origem;

4.8.1.11.13. Deve implementar balanceamento de link por hash do IP de origem e destino;

4.8.1.11.14. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

4.8.1.11.15. Deve suportar o balanceamento de, no mínimo, três links;

4.8.1.11.16. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

4.8.1.11.17. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

4.8.1.11.18. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

4.8.1.11.19. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

4.8.1.11.20. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

4.8.1.11.21. A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

4.8.1.11.22. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

4.8.1.11.23. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

4.8.1.11.24. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

4.8.1.11.25. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc.;

4.8.1.11.26. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

4.8.1.11.27. O QoS deve possibilitar a definição de fila de prioridade;

4.8.1.11.28. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

4.8.1.11.29. A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

4.8.1.11.30. Deve possibilitar a definição de bandas distintas para download e upload;

4.8.1.11.31. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

4.8.1.11.32. A solução de SD-WAN deve suportar IPv6;

4.8.1.11.33. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

4.8.1.11.34. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.8.1.11.35. O SD-WAN deverá possuir serviço de Firewall Stateful;

4.8.1.11.36. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

4.8.1.11.37. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

4.8.1.11.38. Deve ser capaz de bloquear acesso às aplicações;

4.8.1.11.39. Deve suportar NAT dinâmico bem como NAT de saída;

4.8.1.11.40. Deve suportar balanceamento de tráfego por sessão e pacote;

4.8.1.11.41. Suportar VPN IPSec Site-to-Site;

4.8.1.11.42. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

4.8.1.11.43. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.8.1.11.44. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

4.8.1.11.45. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

4.8.1.11.46. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

4.8.1.11.47. Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;

4.8.1.11.48. Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

4.8.1.11.49. Deve possuir suporte e estar licenciamento para uso de VRFs;

4.8.1.11.50. A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance.

4.8.2. **ITEM 2 - FIREWALL DE PEQUENO PORTE**

4.8.2.1. **Descrições básicas**

4.8.2.1.1. Throughput de, no mínimo, 800 Mbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação, habilitadas simultaneamente;

4.8.2.1.2. Throughput de, no mínimo, 600Mbps para Prevenção de ameaças, considerando Controle de Aplicação, IPS, anti malware e firewall, habilitados simultaneamente;

4.8.2.1.3. Throughput de, no mínimo, 5 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

4.8.2.1.4. Suporte a, pelo menos, 700 mil sessões concorrentes TCP;

4.8.2.1.5. Suporte a, pelo menos, 35 mil novas sessões TCP por segundo;

4.8.2.1.6. Suportar no mínimo 310 Mbps de throughput de Inspeção SSL;

4.8.2.1.7. Throughput de, no mínimo, 1 Gbps de IPS;

4.8.2.1.8. Suporte a, no mínimo, 200 clientes VPN SSL;

4.8.2.1.9. Suporte a, no mínimo, 200 clientes VPN IPsec;

4.8.2.1.10. Possuir ao menos 5 interfaces RJ45 padrão Gigabit Ethernet;

4.8.2.1.11. Suportar a criação de no mínimo 5 instâncias virtuais;

4.8.2.1.12. Possuir alimentação elétrica de corrente alternada padrão 110v/220v;

4.8.2.1.13. Deve estar homologado na ANATEL até a data da licitação;

4.8.2.1.14. Os números acima devem ser comprovados com documentação pública, disponível no site do fabricante.

4.8.2.2. **Características Gerais**

4.8.2.2.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

4.8.2.2.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

4.8.2.2.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.8.2.2.4. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.8.2.2.5. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

4.8.2.2.6. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

4.8.2.2.7. Deve suportar BGP, OSPF, RIP e roteamento estático;

4.8.2.2.8. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

4.8.2.2.9. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

4.8.2.2.10. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;

4.8.2.2.11. Deve suportar ao menos 30 tabelas independentes de roteamento, por contexto de firewall;

4.8.2.2.12. Deve suportar NAT dinâmico (Many-to-Many);

4.8.2.2.13. Deve suportar NAT estático (1-to-1);

4.8.2.2.14. Deve suportar NAT estático bidirecional 1-to-1;

4.8.2.2.15. Deve suportar Tradução de porta (PAT);

4.8.2.2.16. Deve suportar NAT de Origem;

4.8.2.2.17. Deve suportar NAT de Destino;

4.8.2.2.18. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

4.8.2.2.19. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

4.8.2.2.20. Deve suportar NAT64;

4.8.2.2.21. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

4.8.2.2.22. Enviar log para sistemas de monitoração externos;

4.8.2.2.23. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

4.8.2.2.24. Proteção anti-spoofing;

4.8.2.2.25. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

4.8.2.2.26. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.8.2.2.27. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de

4.8.2.2.28. Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

4.8.2.2.29. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

4.8.2.2.30. Controle, inspeção e descriptografia de SSL para tráfego de Saída (Outbound);

4.8.2.2.31. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos e softwares a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

4.8.2.2.32. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

4.8.2.2.33. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI;

4.8.2.2.34. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

4.8.2.2.35. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN.

4.8.2.3. **Políticas**

4.8.2.3.1. Deverá suportar controles por zonas de segurança;

4.8.2.3.2. Deverá suportar controles de políticas por porta e protocolo;

4.8.2.3.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

4.8.2.3.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.8.2.3.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

4.8.2.3.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

4.8.2.3.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

4.8.2.3.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

4.8.2.3.9. Suporte a objetos e regras IPV6;

4.8.2.3.10. Suporte a objetos e regras multicast;

4.8.2.3.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré- definidos automaticamente.

4.8.2.4. **Controle de Aplicações**

4.8.2.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.8.2.4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.8.2.4.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.8.2.4.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, twitter, logmein, teamviewer, ms- rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, dropbox, google drive, ldap, radius, itunes, dhcp, ftp, dns, ntp, snmp, webex, evernote, google-docs; 5.2.4.5 Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.8.2.4.5. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.8.2.4.6. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.8.2.4.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

4.8.2.4.8. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.8.2.4.9. Atualizar a base de assinaturas de aplicações automaticamente;

4.8.2.4.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory/LDAP, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

4.8.2.4.11. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.8.2.4.12. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos;

4.8.2.4.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

4.8.2.4.14. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.8.2.4.15. Deve alertar o usuário quando uma aplicação for bloqueada;

4.8.2.4.16. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle /políticas para os mesmos;

4.8.2.4.17. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

4.8.2.4.18. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo: permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

4.8.2.4.19. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle /políticas para os mesmos;

4.8.2.4.20. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

4.8.2.4.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

4.8.2.4.22. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

4.8.2.4.23. Deve permitir forçar o uso de portas específicas para determinadas aplicações;
Deve permitir o filtro de vídeos que podem ser visualizados no YouTube.

4.8.2.5. **Prevenção de ameaças**

4.8.2.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

4.8.2.5.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.8.2.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.8.2.5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e colocar em quarentena o IP do atacante por um intervalo de tempo;

4.8.2.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.8.2.5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

4.8.2.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.8.2.5.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.8.2.5.9. Deve permitir o bloqueio de vulnerabilidades;

4.8.2.5.10. Deve permitir o bloqueio de exploits conhecidos;

4.8.2.5.11. Deve incluir proteção contra-ataques de negação de serviços;

4.8.2.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

4.8.2.5.13. Detectar e bloquear a origem de portscans;

4.8.2.5.14. Bloquear ataques efetuados por worms conhecidos;

4.8.2.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.8.2.5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.8.2.5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.8.2.5.18. Deve permitir usar operadores lógicos de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

4.8.2.5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.8.2.5.20. Identificar e bloquear comunicação com botnets;

4.8.2.5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.8.2.5.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

4.8.2.5.23. Os eventos devem identificar o país de onde partiu a ameaça;

4.8.2.5.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

4.8.2.5.25. Possuir proteção contra downloads involuntários de arquivos executáveis e maliciosos, usando HTTP;

4.8.2.5.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.8.2.5.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

4.8.2.5.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

4.8.2.5.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

4.8.2.6. **Filtro de URLs**

4.8.2.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.8.2.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

4.8.2.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory/LDAP e base de dados local;

4.8.2.6.4. A identificação pela base do Active Directory/LDAP deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

4.8.2.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

4.8.2.6.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

4.8.2.6.7. Possuir pelo menos 60 categorias de URLs;

4.8.2.6.8. Deve possuir a função de exclusão de URLs do bloqueio;

4.8.2.6.9. Permitir a customização de página de bloqueio;

4.8.2.6.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

4.8.2.6.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário.

4.8.2.7. **Identificação de usuários**

4.8.2.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

4.8.2.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.8.2.7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

4.8.2.7.4. Deve possuir integração com Microsoft Active Directory/LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

4.8.2.7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em usuários e grupos de usuários;

4.8.2.7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em Usuários e Grupos de usuários;

4.8.2.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

4.8.2.7.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.8.2.7.9. Deve suportar o envio e recebimento de credenciais via RADIUS.

4.8.2.8. **Filtro de dados**

4.8.2.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

4.8.2.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.8.2.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.8.2.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

4.8.2.9. **Geolocalização**

4.8.2.9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

4.8.2.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.8.2.10. **VPN Client to Site**

4.8.2.10.1. Suportar IPSec VPN;

4.8.2.10.2. Suportar SSL VPN;

4.8.2.10.3. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

4.8.2.10.4. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

4.8.2.10.5. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

4.8.2.10.6. Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

4.8.2.10.7. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

4.8.2.10.8. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

4.8.2.10.9. Suportar leitura e verificação de CRL (certificate revocation list);

4.8.2.10.10. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

4.8.2.10.11. A VPN SSL deve permitir aos usuários remotos a troca de senha no Active Directory/LDAP;

4.8.2.10.12. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8.1 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 e superior).

4.8.2.11. **Recursos Gerais de SD-WAN**

4.8.2.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

4.8.2.11.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

4.8.2.11.2.1. Endereços de origem;

4.8.2.11.2.2. Grupos de usuários;

4.8.2.11.2.3. Endereços de destino;

4.8.2.11.2.4. DSCP;

4.8.2.11.2.5. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

4.8.2.11.3. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

4.8.2.11.4. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G;

4.8.2.11.5. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

4.8.2.11.6. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

4.8.2.11.7. A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

4.8.2.11.8. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

4.8.2.11.9. A solução deve permitir a definição do roteamento para cada aplicação;

4.8.2.11.10. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

4.8.2.11.11. Deve possibilitar a definição do link de saída para uma aplicação específica;

4.8.2.11.12. Deve implementar balanceamento de link por hash do IP de origem;

4.8.2.11.13. Deve implementar balanceamento de link por hash do IP de origem e destino;

4.8.2.11.14. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

4.8.2.11.15. Deve suportar o balanceamento de, no mínimo, três links;

4.8.2.11.16. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

4.8.2.11.17. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

4.8.2.11.18. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

4.8.2.11.19. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

4.8.2.11.20. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

4.8.2.11.21. A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

4.8.2.11.22. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

4.8.2.11.23. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

4.8.2.11.24. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

4.8.2.11.25. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc.;

4.8.2.11.26. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

4.8.2.11.27. O QoS deve possibilitar a definição de fila de prioridade;

4.8.2.11.28. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

4.8.2.11.29. A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

4.8.2.11.30. Deve possibilitar a definição de bandas distintas para download e upload;

4.8.2.11.31. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

4.8.2.11.32. A solução de SD-WAN deve suportar IPv6;

4.8.2.11.33. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

4.8.2.11.34. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.8.2.11.35. O SD-WAN deverá possuir serviço de Firewall Stateful;

4.8.2.11.36. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

4.8.2.11.37. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

4.8.2.11.38. Deve ser capaz de bloquear acesso às aplicações;

4.8.2.11.39. Deve suportar NAT dinâmico bem como NAT de saída;

4.8.2.11.40. Deve suportar balanceamento de tráfego por sessão e pacote;

4.8.2.11.41. Suportar VPN IPSec Site-to-Site;

4.8.2.11.42. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

4.8.2.11.43. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.8.2.11.44. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

4.8.2.11.45. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

4.8.2.11.46. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

4.8.2.11.47. Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;

4.8.2.11.48. Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

4.8.2.11.49. Deve possuir suporte e estar licenciamento para uso de VRFs;

4.8.2.11.50. A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance.

4.8.3. **ITEM 3 - ANALISADOR DE TRÁFEGO, ARMAZENAMENTO DE LOG E RELATÓRIOS**

4.8.3.1. Deve ser do mesmo fornecedor da solução de NGFW ofertada, bem como suportar a base atual da UFU, composta de firewalls FortiGate e gerência FortiManager.

4.8.3.2. A solução deverá ser entregue no formato appliance físico;

4.8.3.3. A solução deve suportar armazenamento de ao menos 8 TB de área útil após a confecção do RAID;

4.8.3.4. A solução deve suportar no mínimo o envio diário de 200GBytes de logs por dia;

4.8.3.5. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.8.3.6. O sistema deverá suportar contas de usuário/senha estáticas;

4.8.3.7. Permitir acesso concorrente de administradores;

4.8.3.8. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.8.3.9. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius;

4.8.3.10. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC;

4.8.3.11. A comunicação com os firewalls gerenciados deve ser protegida e criptografada;

4.8.3.12. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;

4.8.3.13. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

4.8.3.14. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência.

4.8.3.15. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;

4.8.3.16. Deve oferecer portal personalizado para gerenciamento de dispositivos, políticas e objetos, junto com painéis, relatórios e visualizações personalizadas para atualizações de segurança abrangentes, análises em tempo real e respostas exclusivas às suas necessidades;

4.8.3.17. Deve permitir a correlação de eventos, provendo dashboards diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

4.8.3.18. O portal deve permitir uma visão geral do tráfego de rede e da postura de segurança, incluindo widgets intuitivos com informações como principais países, principais ameaças, principais origens de tráfego, principais destinos, principais aplicativos e hits de políticas, bem como gráficos para mostrar logins de administrador, eventos do sistema, e uso de recursos;

4.8.3.19. O portal deve suportar a sua configuração possibilite seu uso via multi-tenant, ou seja, com a possibilidade de se criar vários portais de acesso independentes entre si para fins de administração distribuída;

4.8.3.20. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura etc.;

4.8.3.21. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

4.8.3.22. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

4.8.3.23. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

4.8.3.24. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

4.8.3.25. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

4.8.3.26. Deve possuir mecanismos de remoção automática para logs antigos;

4.8.3.27. Permitir importação e exportação de relatórios;

4.8.3.28. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

4.8.3.29. Deve permitir exportar os logs no formato CSV;

4.8.3.30. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

4.8.3.31. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

4.8.3.32. A solução deve ter relatórios predefinidos;

4.8.3.33. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

4.8.3.34. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

4.8.3.35. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

4.8.3.36. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

4.8.3.37. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

4.8.3.38. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

4.8.3.39. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

4.8.3.40. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

4.8.3.41. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

4.8.3.42. Permitir o envio por e-mail relatórios automaticamente;

4.8.3.43. Deve permitir que o relatório seja enviado por email para o destinatário específico;

4.8.3.44. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

4.8.3.45. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

4.8.3.46. Deve permitir o uso de filtros nos relatórios;

4.8.3.47. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

4.8.3.48. Permitir especificar o idioma dos relatórios criados;

4.8.3.49. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

4.8.3.50. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

4.8.3.51. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

4.8.3.52. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

4.8.3.53. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

4.8.3.54. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

4.8.3.55. Deve permitir visualizar em tempo real os logs recebidos;

4.8.3.56. Deve permitir o encaminhamento de log no formato syslog;

4.8.3.57. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

4.8.3.58. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

4.8.3.59. Deve permitir gerar alertas de eventos a partir de logs recebidos.

4.8.4. **Equipamentos Fortinet que atendem especificações**

4.8.4.1. Nesta seção apresentamos os equipamentos do fabricante Fortinet que atendem a configuração mínima detalhada nas subseções

4.8.4.1.1. ***Firewall de médio porte: FG-101F + UTP (Unified Threat Protection) 5 anos***

4.8.4.1.2. ***Firewall de pequeno porte: FG-40F + UTP (Unified Threat Protection) 5 anos***

4.8.4.1.3. ***Analisador de tráfego, armazenamento de logs e relatórios: FAZ-800G + Forticare 5 anos***

4.8.5. **Soluções alternativas**

4.8.5.1. Considerando que os equipamentos já adquiridos e atualmente em operação são do fabricante Fortinet, é essencial que os equipamentos objetos deste processo licitatório sejam do mesmo fabricante. Atém disso, do ponto de vista técnico, o equipamento de gerência centralizada atualmente em produção em nossa infraestrutura (FortiManager 200F) não é capaz de operar firewalls de outro fabricante. Por fim, este requisito também é necessário para compatibilidade e operação junto à solução para análise de tráfego.

4.8.5.2. Caso algum fornecedor queira ofertar produtos de outro fabricante, o mesmo deverá substituir, sem custo, a base atual da instituição, composta de 2 (dois) equipamentos FortiGate 1500D (com licenciamento de software e hardware completo), 1 (um) equipamento FortiGate 201E (com licenciamento de software e hardware completo) e 1 (um) equipamento FortiManager 200F (com licenciamento de software e hardware completo). Os modelos ofertados devem possuir capacidade igual ou superior aos equipamentos citados e serem todos do mesmo fabricante. Além disso, o fornecedor deverá ofertar, sem custo, treinamento oficial do fabricante com duração mínima de 80 horas e emissão de certificado de conclusão emitido pelo fabricante dos equipamentos.

4.9. **Requisitos de Projeto e de Implementação**

4.9.1. O bem a ser adquirido será solicitado junto ao vencedor do certame, conforme as necessidades demandadas.

4.9.2. Será avaliada a compatibilidade do item quanto às especificações elencadas neste Termo, a fim de assegurar a implementação imediata da solução de TIC contratada.

4.10. **Requisitos de Garantia**

4.10.1. Todos os equipamentos/softwares fornecidos deverão ser novos, de primeiro uso e estarem na linha de produção atual do fabricante;

4.10.2. Todos os componentes de hardware da solução deverão ser de um único fabricante ou em regime de OEM, não sendo permitida a integração de itens não homologados (ex.: memórias e discos rígido) de terceiros que venha a ocasionar perda parcial ou total da garantia ou qualquer ônus financeiro adicional durante a vigência da garantia;

4.10.3. O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto;

4.10.4. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante;

4.10.5. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas;

4.10.6. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias;

4.10.7. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento;

4.10.8. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 1 (um) dia útil;

4.10.9. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante;

4.10.10. Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos;

4.10.11. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da Contratada o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos;

4.10.12. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada;

4.10.13. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual;

4.10.14. A garantia e suporte deverão ser prestados em regime de 24 (vinte e quatro) horas, 07 (sete) dias por semana com tempo de atendimento no próximo dia útil (NBD);

4.10.15. Os serviços de reparo dos equipamentos especificados serão executados somente e exclusivamente onde se encontram (ON-SITE);

4.10.16. O fabricante deve possuir central de atendimento por meio de atendimento telefônico, sistema web de help-desk (sistema de chamados) e e-mail, com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema e permitindo consulta em tempo real aos registros;

4.10.17. Durante todo o período de garantia, a assistência técnica será prestada pelo fabricante com atendimento por mão de obra treinada e especializada;

4.10.18. Todos os equipamentos e suas funcionalidades descritas neste documento deverão ser fornecidos em pleno funcionamento e sem restrições de licenciamento;

4.10.19. A garantia deverá incluir a disponibilização de todas as atualizações de softwares e firmwares dos equipamentos, sem qualquer ônus adicional para a contratante;

4.10.20. As atualizações devem ser do tipo “minor release” e “major release”, permitindo a correção de vícios e para manter os softwares e firmwares de equipamentos atualizados em sua última versão;

4.10.21. Deverá ser garantido o acesso a drivers, manuais e softwares, obrigatoriamente durante o período de garantia e até que o fabricante descontinue o suporte ao equipamento;

4.10.22. Tal acesso deve ser realizado via site dos fabricantes dos equipamentos e softwares, devendo permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

4.11. Requisitos de Experiência Profissional

4.11.1. A Diretoria do Centro de Tecnologia da Informação e Comunicação, representada pela Diretoria de Infraestrutura e Suporte ao Usuário designará equipe, composta por Analistas e Técnicos de TI para executar a implantação a solução.

4.12. Requisitos de Metodologia de Trabalho

4.12.1. A metodologia de trabalho se baseia no acompanhamento da demanda, desde a sua solicitação até a entrega do produto.

4.13. Requisitos de Segurança da Informação

4.13.1. A empresa a ser contratada deverá atender às normas acerca de conformidade técnica e de integridade de dados na Administração Pública Federal, bem como os demais atos, documentos e normativos expedidos e publicados pela Administração Pública Federal relativos à segurança e à privacidade das informações e comunicações.

4.13.2. As formas de acesso e critérios de Segurança da Informação obedecerão à Política de Segurança da Informação da CONTRATANTE. A CONTRATADA deverá tratar como informações sigilosas e privadas da CONTRATANTE quaisquer dados ou informações disponíveis em componentes dos equipamentos ou softwares, os quais venham a ter acesso em função da prestação de serviços, não podendo revelá-los ou facilitar seu acesso a terceiros.

4.13.3. A fim de obter comprometimento formal sobre o sigilo dos dados e informações de uso da CONTRATANTE, bem como suas normas e políticas de segurança, a CONTRATADA deverá concordar e assinar, por meio de representante legal, o Termo de Compromisso.

5. RESPONSABILIDADES

5.1. Deveres e responsabilidades da contratante

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos.

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico.

5.1.3. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas.

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis.

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC.

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável.

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração.

5.2. **Deveres e responsabilidades da contratada**

5.2.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, conforme Lei nº 8.666/93 e demais normas legais e regulamentares pertinentes, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

5.2.2. Efetuar o fornecimento do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade.

5.2.3. Realizar a entrega dos bens conforme prazo estabelecido neste Termo de Referência, a contar da assinatura do contrato ou do recebimento da Nota de Empenho.

5.2.4. Entregar os bens adquiridos sempre acompanhados dos respectivos manuais técnico-operacionais, redigidos em português e relação da rede de assistência técnica autorizada.

5.2.5. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os arts. 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

5.2.6. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato.

5.2.7. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

5.2.8. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante.

5.2.9. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária.

5.2.10. Manter, durante toda a execução do contrato, as mesmas condições da habilitação.

5.2.11. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC.

5.2.12. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato.

5.2.13. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a

documentação, os modelos de dados e as bases de dados à Administração.

5.2.14. Proceder à entrega dos bens, devidamente embalados, de modo a não serem danificados durante a operação de transporte e de carga e descarga, identificando na embalagem a marca, destino, validade e procedência. Quando for o caso, número da licença de importação ou documento equivalente, com as especificações detalhadas para conferência.

5.2.15. Comunicar à contratante por escrito e em tempo hábil, qualquer anormalidade que esteja impedindo a execução contratual, prestando os esclarecimentos julgados necessários.

5.2.16. Substituir todo e qualquer bem fornecido com defeito ou fora do padrão contratado, ou ainda apresentar defeito durante o prazo de garantia.

5.2.17. Realizar testes e corrigir defeitos nos bens, inclusive com a sua substituição, quando necessário, sem ônus para a contratante, durante o período de garantia.

5.2.18. Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os bens fornecidos, bem como pelo custo do frete e outros inerentes a execução do objeto, apresentando os documentos fiscais dos produtos com a legislação vigente.

5.2.19. Responsabilizar-se pela fiel execução contratual, respondendo civil e criminalmente pelos danos, perdas ou prejuízos que, por dolo ou culpa sua ou de seus empregados, causarem a contratante ou a terceiros, sendo admitindo o direito à ampla defesa.

5.2.20. A contratada deverá atender, no que couber, os critérios de sustentabilidade ambiental previstos na Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010.

5.2.21. Manter, durante toda a vigência da Ata de Registro de Preços, as condições de habilitação e qualificações exigidas para a contratação.

5.3. **Deveres e responsabilidades do órgão gerenciador da ata de registro de preços**

5.3.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões, constam da minuta de Ata de Registro de Preços.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. **Vigência**

6.1.1. As regras referentes à Ata de registro de preços, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

6.2. **Rotinas de Execução**

6.2.1. Os materiais deverão ser fornecidos após o recebimento da ordem de fornecimento em até 60 (sessenta) dias.

6.2.2. O local de entrega será no endereço da Divisão de Recepção, Armazenagem e Distribuição de Equipamentos da Universidade Federal de Uberlândia, na Av. Amazonas, 2210 - Bloco 2Z - Sala(s) DIRAM - Bairro Umuarama - Campus Umuarama - Uberlândia-MG - CEP 38405-302.

6.3. **Quantidade mínima de bens ou serviços para comparação e controle**

6.3.1. A quantidade mínima a ser entregue será de 1 unidade do objeto.

6.4. **Mecanismos formais de comunicação**

6.4.1. Contato por e-mail institucional da empresa vencedora do certame.

6.4.2. Contato por meio telefônico em uma central de atendimento oferecida pela empresa.

6.4.3. Utilização de ordens de serviços, fornecimento de bens, entre outros documentos relacionados.

6.5. **Manutenção de sigilo e normas de segurança**

6.5.1. A contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo contratante a tais documentos.

6.5.2. O Termo de Compromisso deverá conter declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade e ser assinado pelo representante legal da Contratada, e o Termo de Ciência deverá ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. Serão aceitos os equipamentos que estiverem de acordo as especificações técnicas contidas no edital. No ato da entrega dos equipamentos, os mesmos serão verificados e existindo alguma inconformidade, não serão aceitos e sua troca será exigida.

7.1.2. A entrega dos equipamentos deverá estar em conformidade com o pedido formalmente realizado pela Universidade em face da vencedora do certame, de acordo com os critérios, especificações, quantitativos e demais detalhes constantes no contrato e/ou no termo de referência.

7.2. Procedimentos de Teste e Inspeção

7.2.1. Por se tratar de aquisição de equipamentos, os procedimentos de teste e inspeção se basearão em testes de performance, além do acompanhamento durante a utilização dos equipamentos.

7.2.2. Ao receber os equipamentos deverá ser realizada a inspeção para verificar se todos os itens estão sendo entregues pela contratada, considerando os aspectos quantitativos e qualitativos.

7.2.3. Durante a configuração / instalação dos equipamentos, poderão ser feitos testes de performance, utilizando-se de softwares específicos.

7.2.4. Os equipamentos deverão ser utilizados conforme instruções do fabricante e as orientações da contratada, reduzindo assim os riscos de danos materiais.

7.2.5. As requisições de suporte / manutenção aos equipamentos deverão ser acompanhadas com o intuito de se verificar a qualidade dos equipamentos, além da sua vida útil.

7.3. Níveis Mínimos de Serviço Exigidos

IAE - INDICADOR DE ATRASO DE ENTREGA DE OS	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na ordem de fornecimento.
Meta a cumprir	**IAE <= 0** - A meta definida visa garantir a entrega dos produtos e serviços constantes nas ordens de fornecimento dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da contratante e lista de termos de recebimento provisório e definitivo emitidos.
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na ordem de fornecimento.
Periodicidade	Para cada ordem de fornecimento encerrada e com termo de recebimento definitivo.

Mecanismo de Cálculo (métrica)	**IAE = $\frac{TEX - TEST}{TEST}$** Onde: **IAE** – Indicador de Atraso de Entrega; **TEX** – Tempo de Execução – corresponde ao período de execução da ordem de fornecimento, da sua data de início até a data de entrega dos produtos. A data de início será aquela contante na ordem de fornecimento; caso não esteja explícita, será o primeiro dia útil após a emissão da ordem de fornecimento. A data de entrega da ordem de fornecimentodeverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no termo de referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da ordem continua a correr, findando-se apenas quando a contratada entrega os produtos e haja aceitação por parte do fiscal técnico. **TEST** – Tempo Estimado para a execução da ordem de fornecimento, conforme estipulado no termo de referência.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da contratante.
Início de Vigência	A partir da emissão da ordem de fornecimento.
Faixas de ajuste no pagamento e sanções	Para valores do indicador **IAE**: De 0 a 0,10 – Pagamento integral da ordem de fornecimento; De 0,11 a 0,20 – Glosa de 1% sobre o valor da ordem de fornecimento; De 0,21 a 0,30 – Glosa de 2% sobre o valor da ordem de fornecimento; De 0,31 a 0,50 – Glosa de 3% sobre o valor da ordem de fornecimento; De 0,51 a 1,00 – Glosa de 4% sobre o valor da ordem de fornecimento; Acima de 1 – Será aplicada Glosa de 5% sobre o valor da ordem de fornecimento e multa de 5% sobre o valor do contrato.

7.4. **Sanções Administrativas e Procedimentos para Retenção ou Glosa**

7.4.1. Comete infração administrativa nos termos de Lei nº 10.520, de 2002, a Contratada que:

7.4.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

7.4.1.2. Ensejar o retardamento da execução do objeto;

7.4.1.3. Falhar ou fraudar na execução do contrato;

7.4.1.4. Comportar-se de modo inidôneo;

7.4.1.5. Cometer fraude fiscal;

7.4.2. Pela inexecução total ou parcial do objeto, a Administração poderá aplicar à contratada as seguintes sanções:

7.4.2.1. Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a contratante;

7.4.2.2. Multa moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;

7.4.2.3. Multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

7.4.2.4. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

7.4.2.5. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

7.4.2.6. Impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos. A sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 7.4. deste termo de referência;

7.4.2.7. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir a contratante pelos prejuízos causados.

7.4.3. As sanções previstas poderão ser aplicadas à contratada juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

7.4.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

7.4.4.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

7.4.4.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

7.4.4.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

7.4.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

7.4.6. As multas devidas e/ou prejuízos causados à contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

7.4.7. Caso a contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.8. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

7.4.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.4.10. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração

da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

7.4.11. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

7.4.12. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.4.13. As penalidades serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores - SICAF.

Id	Ocorrência	Glosa / Sanção
1	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 10% do valor da contratação.
2	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A contratada será declarada inidônea para licitar e contratar com a Administração.
3	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da rescisão contratual.
4	Não executar total ou parcialmente o fornecimento de bens ou serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da rescisão contratual.
5	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, o fornecimento dos bens ou serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do contrato.	Multa de 10% sobre o valor total do contrato. Em caso de reincidência, configura-se inexecução total do contrato por parte da empresa, ensejando a rescisão contratual unilateral.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, o fornecimento dos bens ou serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da rescisão contratual.
7	Não prestar os esclarecimentos imediatamente, referente à execução do objeto da contatação, salvo quando implicarem em indagações de caráter técnico,	Multa de 10% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 5

	hipótese em que serão respondidos no prazo máximo de 24 horas úteis.	dias úteis. Após o limite de 5 dias úteis, aplicar-se-á multa de 10% do valor total do contrato.
8	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega).	Para valores do indicador **IAE**: De 0 a 0,10 – Pagamento integral da ordem de fornecimento; De 0,11 a 0,20 – Glosa de 1% sobre o valor da ordem de fornecimento; De 0,21 a 0,30 – Glosa de 2% sobre o valor da ordem de fornecimento; De 0,31 a 0,50 – Glosa de 3% sobre o valor da ordem de fornecimento; De 0,51 a 1,00 – Glosa de 4% sobre o valor da ordem de fornecimento; Acima de 1 – Será aplicada Glosa de 5% sobre o valor da ordem de fornecimento e multa de 5% sobre o valor do contrato.
9	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 15% do valor total do contrato.

7.5. **Do Pagamento**

7.5.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

7.5.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

7.5.3. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

7.5.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta online ao SICAF ou, na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.5.5. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.6. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a contratante.

7.5.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

7.5.8. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

7.5.9. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

7.5.10. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.11. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.5.12. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

7.5.13. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

7.5.14. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

7.5.15. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

7.5.16. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

7.5.17. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) I = (6/100) / 365

I = 0,00016438

TX= Percentual da taxa anual = 6%

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. A estimativa de preço da contratação foi realizada de acordo com a Instrução Normativa SLTI/MP nº 5, de 27 de junho de 2014, e suas atualizações conforme pode ser verificado por meio do Estudo Técnico Preliminar e seus anexos, todos constantes do processo sob o número SEI 23117.046776/2022-88.

8.2. O custo total estimado da contratação é de R$ 2.012.042,56 (dois milhões, doze mil, quarenta e dois reais e cinquenta e seis centavos), o qual corresponde à média das cotações obtidas.

8.3. No preço cotado e contratado já estão incluídos: impostos, contribuições, taxas, frete, transporte e, se houver, seguro, bem como todos os demais encargos incidentes.

Id.	Descrição do bem ou serviço	Quantidade	Unidade de medida	Valor unitário máximo	Valor total máximo
1	Firewall de médio porte com suporte e garantia de 60 meses	11	Unidade	R$ 133,803.95	R$ 1.471.843,50
2	Firewall de pequeno porte com suporte e garantia de 60 meses	12	Unidade	R$ 17.603,87	R$ 211.246,44
3	Analisador de tráfego, armazenamento de log e relatórios com suporte e garantia de 60 meses	1	Unidade	R$ 328.952,62	R$ 328.952,62

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. A fonte de recursos será informada pela Diretoria de Orçamentos em documento anexo ao processo.

10. DA VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência da contratação, conforme Carta Contrato, será o último dia do prazo exigido para a garantia contratual.

11. DO REAJUSTE DE PREÇOS

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. **Regime, Tipo e Modalidade da Licitação**

12.1.1. O certame licitatório será realizado por meio de Sistema de Registro de Preços, na modalidade Pregão, em sua forma eletrônica, de acordo com o Decreto nº 7.174, de 2010, em seu artigo 9º, §1º. O tipo de licitação será o de menor preço global, em conformidade com a lei mencionada e com a Resolução SEPLAG nº 429/2011.

12.1.2. A opção de utilizar Sistema de Registro de Preços justifica-se pela aquisição de bens com previsão de entregas parceladas, nos moldes do inciso II do art. 3º do Decreto nº 7.892/2013. Conforme a demanda e etapas apresentadas no subitem 3.3, busca-se interrupção mínima dos serviços e sistemas em operação bem como a adequação das atividades à força de trabalho disponível no Centro de Tecnologia da Informação e Comunicação (CTIC). Assim, as entregas dependem da disponibilidade do órgão para fazer as instalações.

12.1.3. A fundamentação pauta-se ainda na premissa que a contratação de serviços ou produtos de tecnologia baseia-se em padrões de desempenho e qualidade claramente definidos no termo de referência, havendo diversos fornecedores capazes de prestá-los. Caracterizando-se como “bem comum” conforme Art. 9º, §2º do Decreto 7.174/2010.

12.1.4. É obrigatória a utilização da modalidade Pregão para as contratações de que trata esta Instrução Normativa sempre que a solução de TIC for enquadrada como bem ou serviço comum, conforme o disposto no § 1º, art. 9º do Decreto nº 7.174, de 2010.

12.1.5. O regime da execução dos contratos é o de preço global, e o tipo e critério de julgamento da licitação é o menor preço para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

12.1.6. De acordo com a IN nº 01, de 4 de abril de 2019, em seu art. 12, § 4º, temos: Nas licitações por preço global, cada serviço ou produto do lote deverá estar discriminado em itens separados nas

propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 3º, § 5º da Lei nº 8.666, de 1993.

12.1.7. Optou-se por agrupar todos os itens em um único lote, pois considerando que fazem parte de um projeto único, é inviável a transferência de tecnologia por mais de uma empresa. Ademais, haveria conflito de prazos no processo de implantação, bem como nos prazos de garantia. Cabe ressaltar ainda, que quando há mais de uma empresa envolvida no processo, dificulta-se o processo de suporte.

12.2. **Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência**

12.2.1. Será observada a aplicabilidade do Direito de Preferência previsto no Decreto nº 7.174/2010 e Lei Complementar nº 123/2006, desde que as EPPs e MEs, atendam aos requisitos legais e aos itens que serão licitados.

12.3. **Critérios de Qualificação Técnica para a Habilitação**

12.3.1. Para a definição dos critérios técnicos para seleção do fornecedor, deverão ser observados:

12.3.1.1. a utilização de critérios correntes no mercado;

12.3.1.2. a necessidade de justificativa técnica nos casos em que não seja permitido o somatório de atestados para comprovar os quantitativos mínimos relativos ao mesmo quesito de capacidade técnica;

12.3.1.3. a vedação da indicação de entidade certificadora, exceto nos casos previamente dispostos em normas da Administração Pública;

12.3.1.4. a vedação de exigência, para fins de qualificação técnica na fase de habilitação, de atestado, declaração, carta de solidariedade, comprovação de parceria ou credenciamento emitidos por fabricantes;

12.3.1.5. a vedação de pontuação com base em atestados relativos à duração de trabalhos realizados pelo licitante, para licitações do tipo técnica e preço; e

12.3.1.6. a justificativa dos critérios de pontuação em termos do benefício que trazem para a contratante, para licitações do tipo técnica e preço.

12.3.2. Aplicam-se ainda para a definição da qualificação técnica para a habilitação os dispositivos indicados no Art. 19 da IN nº 01, de 4 de abril de 2019 e, quanto à documentação, o Art. 30 da Lei nº 8.666/93.

12.3.3. **Documentação Habilitatória Complementar:**

12.3.3.1. Para comprovação da aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, a licitante detentora da proposta classificada em primeiro lugar deverá apresentar:

12.3.3.1.1. DECLARAÇÃO da própria empresa, em papel timbrado, garantindo que:

12.3.3.1.1.1. está apta a fornecer, configurar e prestar suporte da solução ofertada;

12.3.3.1.1.2. que manterá, durante toda a vigência da Garantia, pelo menos 1 (um) profissional com certificação técnica compatível com o(s) objeto(s) deste processo, capaz de prestar o suporte em garantia e escalar o chamado ao fabricante conforme necessidade.

12.3.3.1.1.3. tem ciência de que em momento anterior à instalação dos produtos poderá se convocada a comprovar a disponibilidade e formação do profissional acima requerido.

12.3.3.2. A apresentação da Documentação Habilitatória Complementar deverá se dar conforme convocação do(a) Pregoeiro(a), através de ambiente eletrônico.

12.3.3.3. Nos termos do Art. 43, §3.º da Lei 8.666/93, é facultado à Contratante o direito de promover diligência destinada a esclarecer ou complementar os dados informados na presente Seção.

13. DA PARTICIPAÇÃO EM CONSÓRCIO

13.1. Pela natureza e baixa complexidade do objeto, não será permitida participação de licitantes em consórcio.

14. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

14.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria PROPLAD Nº 3264/2022 (3742145).

14.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o termo de Referência ou projeto básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

14.3. **Equipe de planejamento:**

14.3.1. **Integrante Requisitante**: Paulo Rodolfo da Silva Leite Coelho - Diretor de Infraestrutura e Suporte ao Usuário / Centro de Tecnologia da Informação e Comunicação - SIAPE 1690760.

14.3.2. **Integrante Técnico**: Alisson de Oliveira Chaves - Analista de Tecnologia da Informação da Divisão de Redes / Centro de Tecnologia da Informação e Comunicação - SIAPE 1827900.

14.3.3. **Integrante Administrativa**: Amanda Filsner Dias Strack - Assistente em Administração e Coordenadora da Divisão de Administração de Licitações e Contratos / Centro de Tecnologia da Informação e Comunicação - SIAPE 1877304.

14.4. **Autoridade Máxima da área de TIC**: Rafael Pasquini - Diretor Geral do Centro de Tecnologia da Informação e Comunicação - SIAPE 1881747.

15. ANEXOS

15.1. MODELO DE TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

Eu, [NOME COMPLETO], [cargo, função/setor onde trabalha], [nº CPF], declaro estar ciente da habilitação a ser conferida a mim para manuseio das Bases de dados [XXXXX], mantidas pela UNIVERSIDADE FEDERAL DE UBERLÂNDIA, decorrente do Contrato [nº contrato] conforme Processo SEI [nº protocolo].

No tocante às atribuições a mim conferidas, no âmbito do Termo de Compromisso e Manutenção de Sigilo acima referido, comprometo-me a:

1. manusear a base de dados apenas por necessidade de serviço, ou em caso de determinação expressa, desde que legal, de superior hierárquico;
2. manter a absoluta cautela quando da exibição de dados em tela, impressora, ou, ainda, na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;
3. utilizar a base de dados estritamente conforme descrito e definido no instrumento de cooperação para disponibilização de dados;
4. manter sigilo dos dados ou informações sigilosas obtidas por força de minhas atribuições, abstendo-me de revelá-los ou divulgá-los, sob pena de incorrer nas sanções civis e penais decorrentes de eventual divulgação; e
5. Não repassar a outrem a base de dados em formato identificado.

15.2. MODELO DE TERMO DE CIÊNCIA

(Este artefato objetiva obter dos empregados da Contratada diretamente envolvidos no projeto a ciência formal do Termo de Compromisso de Manutenção de Sigilo e das normas de segurança vigentes na Instituição)

Contrato Nº:	

Objeto:			
Gestor do Contrato:		Matr.:	
Contratante (Órgão):			
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.
_____, _____ de _____ de 20_____.

CIÊNCIA	
CONTRATADA **Funcionários**	
_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <*Matr*.>
_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <*Matr*.>
_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <Matr.>
_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <*Matr*.>

_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <*Matr*.>
_____ <*Nome*> Matrícula: <*Matr*.>	_____ <*Nome*> Matrícula: <*Matr*.>

Uberlândia, 28 de setembro de 2022.

Documento assinado eletronicamente por **Paulo Rodolfo da Silva Leite Coelho**, **Diretor(a)**, em 14/10/2022, às 10:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Rafael Pasquini**, **Diretor(a)**, em 14/10/2022, às 10:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alisson Oliveira Chaves**, **Analista de Tecnologia da Informação**, em 14/10/2022, às 10:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Amanda Filsner Dias Strack**, **Coordenador(a)**, em 14/10/2022, às 11:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4000024** e o código CRC **62265D08**.

Referência: Processo nº 23117.046776/2022-88 SEI nº 4000024